XX 银行
信息安全管理办法

第一章 总 则

第一条 为加强 XX 银行 （下称 “本行”）信息安全管理，防范信息技术风险，保障本行计算机网络与信息系统安全和稳定运行， 根据 《中华人民共和国计算机信息系统安全保护条例》 、 《金融机构计算机信息系统安全保护工作暂行规定》等，特制定本办法 。

第二条 本办法所称信息安全管理， 是指在本行信息化项目立项、 建设、 运行、 维护及废止等过程中保障信息及其相关系统、环境、网络和操作安全的一系列管理活动。

第三条 本行信息安全工作实行统一领导和分级管理， 由分管领导负责。 按照 “谁主管谁负责，谁运行谁负责，谁使用谁负责”的原则，逐级落实部门与个人信息安全责任。

第四条 本办法适用于本行。所有使用本行网络或信息资源的其他外部机构和个人均应遵守本办法。

第二章 组织保障

第五条 常设由本行领导、各部室负责人及信息安全员组成的信息安全领导小组，负责本行信息安全管理工作 ，决策信息安全重大事宜。

第六条 各部室、各分支机构应指定至少一名信息安全员，

配合信息安全领导小组开展信息安全管理工作，具体负责信息安全领导小组颁布的相关管理制度及要求在本部室的落实。。

第七条 本行应建立与信息安全监管机构的联系，及时报告各类信息安全事件并获取专业支持。

第八条 本行应建立与外部信息安全专业机构、专家的联系，及时跟踪行业趋势，学习各类先进的标准和评估方法。

第三章 人员管理

第九条 本行所有工作人员根据不同的岗位或工作范围，履行相应的信息安全保障职责。日常员工信息安全行为准则参见《X 银行员工信息安全手册》。

第一节 信息安全管理人员

第十条 本办法所指信息安全管理人员包括本行信息安全领导小组和信息安全工作小组成员。

第十一条 应选派政治思想过硬、具有较高计算机水平的人员从事信息安全管理工作。凡是因违反国家法律法规和本行有关规定受到过处罚或处分的人员，不得从事此项工作。

第十二条 信息安全管理人员每年至少参加一次信息安全相关培训。

第十三条 安全工作小组在如下职责范围内开展信息安全管理工作：

（一）组织落实上级信息安全管理规定，制定信息安全管理制度，协调信息安全领导小组成员工作，监督检查信息安全

管理工作。

（二）审核信息化建设项目中的安全方案，组织实施信息安全保障项目建设。

（三）定期监督网络和信息系统的安全运行状况，检查运行操作、备份、机房环境与文档等安全管理情况，发现问题，及时通报和预警，并提出整改意见。

（四）统计分析和协调处置信息安全事件。

（五） 定期组织信息安全宣传教育活动， 开展信息安全检查、 评估与培训工作。

第十四条 信息安全领导小组成员在如下职责范围内开展工作：

（一）负责本行信息安全管理体系的落实。

（二）负责提出本行信息安全保障需求。

（三）负责组织开展本行信息安全检查工作。

第二节 技术支持人员

第十五条 本办法所称技术支持人员，是指参与本行网络、信息系统、 机房环境等建设、运行、维护的内部技术支持人员和外包服务人员。

第十六条 本行内部技术支持人员在履行网络和信息系统建设和日常运行维护职责过程中，应承担如下安全义务：

（一）不得对外泄漏或引用工作中触及的任何敏感信息。

（二）严格权限访问，未经业务主管部室授权 不得擅自改变系统设置或修改系统生成的任何数据。

（三）主动检查和监控生产系统安全运行状况 ，发现安全隐患或故障及时报告本部室主管领导，并及时响应、处置。

（四）严格操作管理、测试管理、应急管理、 配置管理、变更管理、档案管理等工作制度，做好数据备份工作。

第十七条 外部技术支持人员应严格履行外包服务合同（协议）的各项安全承诺，签署保密协议。提供技术服务期间，严格遵守本行相关安全规定与操作规程。不得拷贝或带走任何配置参数信息或业务数据，不得对外泄漏或引用任何工作信息。

第三节 一般计算机用户

第十八条 本规定所称一般计算机用户是指使用计算机设备的所有人员。

第十九条 一般计算机用户应承担如下安全义务：

（一）及时更新所用计算机的病毒防治软件和安装补丁程序，自觉接受本部室信息安全员的指导与管理。

（二）不得安装与办公和业务处理无关的其他计算机软件和硬件，不得修改系统和网络配置以屏蔽信息安全防护。

（三） 不得在办公用计算机上安装任何盗版或非授权软件。

（四） 未经信息安全管理人员检测和授权，不得将内部网络的计算机转接入国际互联网；不得将个人计算机接入内部网络或私自拷贝任何信息。

第四章 资产管理

第二十条 本行对所有信息资产进行识别、评估相对价值及重要性，建立资产清单并说明使用规则，明确定义信息资产责任人及其职责。细则参见《XX 银行信息资产分类分级管理规定》。

第二十一条 按照信息资产的价值、法律要求及敏感程度和对业务关键程度，分别依据机密性、完整性、可用性三个属性对信息资产进行分类分级，并建立相应的标识和处理制度。

第二十二条 依照信息资产的分类分级采取不同的安全保护措施，制定完善的访问控制策略，防止未经授权的使用。

第二十三条 依据《XX 银行介质管理规范》加强介质管理与销毁操作管理，确保本行数据的可用性、保密性、完整性。

第五章 物理环境安全管理

第一节 机房安全管理

第二十四条 本规定所称机房是指信息系统主要设备放置、运行的场所以及供配电、通信、空调、消防、监控等配套环境设施。

第二十五条 本行机房的信息安全管理由本行本行信息科技部门负责具体实施和落实。

第二十六条 建立机房设施与场地环境监控系统，对机房空调、消防、不间断电源（UPS ） 、供配电、门禁系统等重要设施实行全面监控。

第二十七条 建立健全机房管理制度，并指派专人担任机房

管理员，落实机房安全责任制。机房管理员应经过相关专业培训 ，熟知机房各类设备的分布和操作要领，定期巡查机房，发现问题及时报告。机房管理员负责保管机房建设或改造的所有文档、图纸以及机房运行记录等有关资料，并随时提供调阅。

第二十八条 建立机房定期维修保养制度。易受季节、温度等环境因素影响的设备、已逾保修期的设备、近期维修过的设备等应成为保养的重点。

第二十九条 依据《浙江省农村合作金融机构机房管理指引》进一步规范机房建设、改造和验收过程，落实机房管理。

第三十条 信息安全领导小组负责定期审核机房安全管理落实情况，并保留相应的审核记录和审核结果。

第二节 重要区域安全管理

第三十一条 本章节所指重要区域为：本行信息中心主备机房和运维监控室等区域。本行信息中心负责制定和执行运维监控方面的安全管理制度。

第三十二条 重要区域应严格出入安全管理，安装门禁、视频监视录像系统，实行定时录像监控，并适当配置自动监控报警功能。

第三十三条 所有门禁、视频监视录像系统的信息资料至少保存三个月。

第三节 办公环境安全管理

第三十四条 在本行大楼入口应设置门卫或接待员，负责出入或公共访问区域的物理安全管理和外来人员的出入登记。

第三十五条 本行信息中心楼层设立门禁，加强人员进出管理。

第三十六条 本行信息中心员工应在公共接待区接待外来人员，未经允许，不得私自将外来人员带入办公区域内。

第三十七条 未经允许，严禁在信息中心办公区域内进行摄影、摄像、录音等记录日常办公行为的活动。

第六章 网络安全管理

第一节 网络规划、建设中的安全管理

第三十八条 本行网络信息科技部负责网络和网络安全的统一规划、建设部署、策略配置和网络资源（网络设备、通讯线路、IP 地址和域名等）分配。

第三十九条 按照统一规划和总体部署原则， 由信息科技部组织实施网络建设、 改造工程，工程投产前应通过安全测试与评估。

第四十条 本行网络建设和改造应符合如下基本安全要求：

（一）网络规划应有完整的安全策略，保障网络传输与应用安全。

（二）具备必要的网络监测、跟踪和审计等管理功能。

（三）针对不同的网络安全域，采取必要的安全隔离措施。

（四）能有效防止计算机病毒对网络系统的侵扰和破坏。

第二节 网络运行安全管理

第四十一条 信息科技部应建立健全网络安全运行方面的制度，配备专职网络管理员。网络管理员负责日常监测和检查网络 安全运行状况，管理网络资源及其配置信息，建立健全网络运行维护档案，及时发现和解决网络异常情况。

第四十二条 网络管理员应定期参加网络安全技术培训，具备一定的非法入侵、病毒蔓延等网络安全威胁的应对技能。

第四十三条 严格网络接入管理。任何设备接入网络前，接入方案、设备的安全性等应经过网络管理人员的审核与检测，审 核（检测）通过后方可接入并分配相应的网络资源。

第四十四条 严格网络变更管理。网络管理员调整网络重要参数配置和服务端口时，应严格遵循变更管理流程。实施有可能影响网络正常运行的重大网络变更，应提前通知相关业务部门并安排在非交易时间或交易较少时间进行，同时做好配置参数的备份和应急恢复准备。

第四十五条 严格远程访问控制。确因工作需要进行远程访问的人员应向信息简科技部提出书面申请，并采取相应的安全防护措施。

第四十六条 信息安全管理人员负责定期对网络进行安全检测、扫描和评估。检测、扫描和评估结果属敏感信息，不得向外 界提供。未经授权，任何外部单位与人员不得检测、扫描本行网络。

第三节 接入国际互联网管理

第四十七条 信息科技部负责制定本行互联网方面管理制

度，对互联网接入进行严格的控制，防范来自互联网的威胁。

第四十八条 本行内部业务网、办公网与国际互联网实行安全隔离。所有接入内部网络或存储有敏感工作信息的计算机，不得直接或间接接入国际互联网。

第四十九条 内部网络计算机严禁接入国际互联网，确有必要接入国际互联网的应通过信息安全工作小组审核并上报相关领导审批，确保安装有指定的防病毒软件和最新补丁程序。经审批后连接国际互联网 的计算机，不得存留涉密金融数据信息；存有涉密金融数据信息的介质，不得在接入国际互联网的计算机上使用。

第五十条 曾接入国际互联网的计算机严禁接入内部网络，确有必要接入内部网络的应通过安全工作小组审核并上报相关领导审批， 经安全检测后方能接入。从国际互联网下载的任何信息，未经病毒检测不得在内部网络上使用。

第五十一条 使用国际互联网的所有用户应遵守国家有关法律法规和本行相关管理规定，不得从事任何违法违规活动。

第七章 访问控制

第五十二条 本行负责建立访问控制制度，对信息资产和服务的访问和权限分配进行控制。

第五十三条 信息资产的责任人负责确定信息资产和服务的访问权限，运行维护科根据授权进行相关设定操作。

第五十四条 信息系统用户设置本人的用户和密码， 并对

其访问控制权限负责。重要信息系统操作人员的密码应由系统管理员和业务部门负责人分段设立。

第五十五条 凡是能够执行录入、复核制度的信息系统，操作人员不得一人兼录入、复核两职。未经主管领导批准，不得代岗、兼岗。

第五十六条 应启用安全措施限制授权用户对操作系统的访问， 包括但不限于：

（一）按照已定义的访问控制策略鉴别授权用户；

（二）记录成功和失败的系统访问企图；

（三）记录专用系统特殊权限的使用情况；

（四）当违反系统安全策略时发布警报；

（五）提供合适的身份鉴别手段；

（六）限制用户的连接时间。

第五十七条 对应用系统和信息的逻辑访问应只限于已授权的用户。对应用系统的访问控制措施包括但不限于：

（一）按照定义的访问控制策略，控制用户访问信息和应用系统的特定功能；

（二）防止能够绕过系统控制或应用控制的任 何实用程序、系统软件和恶意软件对系统进行未授权访问；

（三）为重要的敏感系统设立隔离的运行环境。

第五十八条 访问控制实施细则详见 《X 银行信息系统访问控制管理规定》。

第八章 信息系统安全管理

第五十九条 本规定所指的信息系统是本行业务处理系统、管理信息系统和日常办公自动化系统等，包括数据库、软件和硬件支撑环境等。

第六十条 信息系统安全管理实施细则详见《X 银行计算机信息系统安全管理规定》。

第一节 信息系统规划与立项

第六十一条 信息系统建设项目应在规划与立项阶段同步考虑安全问题，建设方案应满足信息安全管理的相关要求。项目技术方案应包括以下基本安全内容：

（一）业务需求部室提出的安全需求。

（二）安全需求分析和实现。

（三）运行平台的安全策略与设计。

第六十二条 信息安全领导小组负责派遣相关部室安全员对项目技术方案进行安全专项审查并提出审查意见，未通过安全审核的项目不得予以立项。

第二节 信息系统开发与集成

第六十三条 信息系统开发应符合软件工程规范，依据安全需求进行安全设计，保证安全功能的完整实现。

第六十四条 信息系统开发单位应在完成开发任务后将程序源代码及相关技术资料全部移交本行。外部开发单位还应与本行签署相关知识产权保护协议和保密协议，不得将信息系统采用的关键安全技术措施和核心安全功能设计对外公开。

第六十五条 信息系统的开发人员不能兼任信息系统管理员或业务系统操作人 员，不得在程序代码中植入后门和恶意代码程序。

第六十六条 信息系统开发、测试、修改工作不得在生产环境中进行。

第六十七条 涉密信息系统集成应选择具有国家相关部门颁发的涉密系统集成资质证书的单位或企业，并签订严格的保密协议。

第六十八条 系统上线前应开展代码审计过程检查源代码中的缺点和错误信息，避免引发安全漏洞。

第三节 信息系统运行

第六十九条 信息系统上线运行实行安全审查机制，未通过安全审查的任何新建或改造信息系统不得投产运行。具体要求如下：

（一）项目承建单位（部室）应组织制定安全测试方案，进行系统上线前的自测试并形成测试报告，报信息科技部审查。

（二）信息系统归口责任业务部室应在信息系统投产运行前同步制定相关安全操作规定，报信息科技部门。

（三）信息科技部应提出明确的测试方案和测试报告审查意见。必要时，可组织专家评审或实施信息系统漏洞扫描检测。

第七十条 信息系统投入使用前信息中心应当建立相应的操